

A simple chaotic circuit with a hyperbolic sine function and its use in a sound encryption scheme

Christos Volos  · Akif Akgul · Viet-Thanh Pham ·
Ioannis Stouboulos · Ioannis Kyprianidis

Received: 15 November 2016 / Accepted: 23 March 2017
© Springer Science+Business Media Dordrecht 2017

Abstract In this work, one of the most simple chaotic autonomous circuits, which has been reported in the literature, is presented. The proposed circuit, that belongs to jerk systems family, is described mathematically by a 3-D dynamical system with only five terms, and it has only one nonlinear term, which is the hyperbolic sine term implemented with two antiparallel diodes. This new jerk system presents interesting chaotic phenomena, such as coexisting attractors and antimonotonicity. Also, as an application of the proposed system a sound encryption scheme that is based on a random number generator, which is implemented with the jerk system, is presented. The practical usefulness of the proposed simple chaotic jerk circuit is confirmed from the results of NIST-800-22 tests of the chaotic random

number generator, as well as from the successful sound encryption and decryption process.

Keywords Nonlinear circuit · Chaos · Antimonotonicity · Coexisting attractors · Random number generator · NIST-800-22 · Sound encryption

1 Introduction

In the last decades, chaotic circuits have received considerable interest in the research community due to the fact that they have been applied in numerous areas such as in electronic circuits' design, secure communications, neural networks, robotics, image processing, random bit generator or emulating economical models [1–30]. For this reason, a great number of chaotic systems, which are circuitry implemented, have been reported in the literature. However, one of the most important research directions is the construction of robust chaotic oscillators with as simple as possible structure from a circuitry or a mathematical point of view.

Concerning the first direction, many simple autonomous or nonautonomous nonlinear chaotic circuits have been presented. Some typical discovered examples of simple nonautonomous chaotic oscillators are Linsay's anharmonic oscillator with a resistor, an inductor, and a varactor diode [31]; Dean's circuit with a capacitor, a linear resistor, and a resistor including ohmic losses in the inductor winding [32]; Laksh-

Electronic supplementary material The online version of this article (doi:[10.1007/s11071-017-3499-9](https://doi.org/10.1007/s11071-017-3499-9)) contains supplementary material, which is available to authorized users.

C. Volos (✉) · I. Stouboulos · I. Kyprianidis
Physics Department, Aristotle University of Thessaloniki,
54124 Thessaloniki, Greece
e-mail: volos@physics.auth.gr

A. Akgul
Department of Electrical and Electronics Engineering,
Faculty of Technology, Sakarya University,
54187 Serdivan, Sakarya, Turkey

V.-T. Pham
School of Electronics and Telecommunications, Hanoi
University of Science and Technology, 01 Dai Co Viet, Hanoi,
Vietnam

manan's sinusoidally driven second-order circuit with three linear elements and a Chua's diode [33]; or Lindberg's chaotic oscillator with a transistor, two capacitors, and two resistors [34]. In the realm of simple autonomous chaotic oscillators, noticeable examples are Hartley's oscillator based on a junction field effect transistor and a tapped coil [35]; two-element memristive time-delay system [36]; three-element circuit with a nonlinear active memristor [37]; four-element Chua's circuit [38]; simple current-tunable chaotic oscillators using floating or virtually grounded diodes [39]; RLCC-Diode-Opamp chaotic oscillator with six electronic components [40]; Piper's circuits using only op-amps and linear time-invariant passive components [41]; or Tamasevicius' oscillator consisting of an op-amp, an LCR resonance loop, an extra capacitor, a diode as a nonlinear element and three auxiliary resistors [42].

Concerning the construction of simple dynamical systems with simple mathematical description is still an open research direction. Although the Lorenz system [43] is often taken as the prototypical chaotic flow, which is a 3-D dynamical system with seven terms in the right-hand side of equations, two of which are nonlinear, it is not the algebraically simplest such system. In 1976, Rössler [44] proposed the well-known system, which also has seven terms but only a single quadratic nonlinearity. The same researcher, three years later, has announced an even simpler 3-D system which has only six terms, a single quadratic nonlinearity and two parameters [45]. Also, unaware of the simpler Rössler example, Sprott [46] embarked on an extensive search for autonomous 3-D chaotic systems with fewer than seven terms and a single quadratic nonlinearity, as well as systems with fewer than six terms and two quadratic nonlinearities. As a result, he found fourteen algebraically distinct cases with six terms and one nonlinearity, and five cases with five terms and two nonlinearities. One case was conservative, and all the others were dissipative, implying the existence of a strange attractor.

Sprott continuing his efforts embarked on an extensive numerical search for chaos in systems of the explicit form $\ddot{x} = J(\ddot{x}, \dot{x}, x)$, ($\dot{x} = y$, $\dot{y} = z$), which it called a "jerk function" since it involves a third derivative of x , which in a mechanical system is the rate of change of the acceleration, sometimes called the "jerk" [47]. He found a variety of cases [48], including two with three terms and two quadratic nonlinearities in

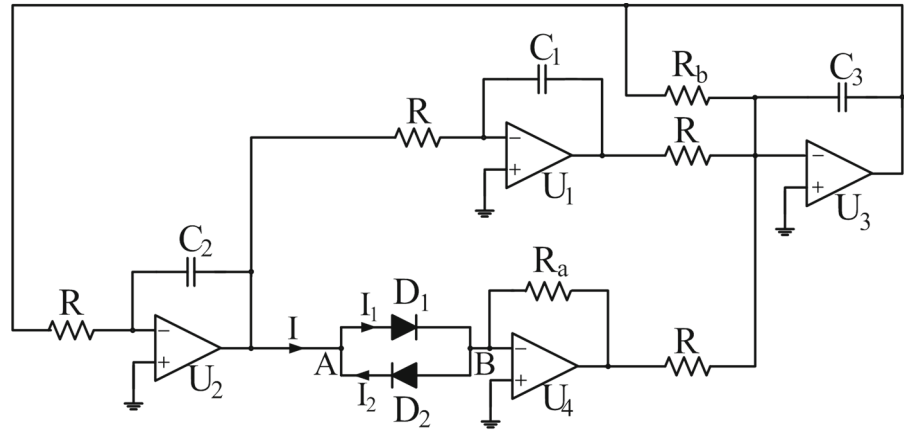
their jerk function, as well as a particularly simple case with three terms and a single quadratic nonlinearity [49],

$$\ddot{x} = -x - a\dot{x} \pm \dot{x}^2 \quad (1)$$

Equation (1) is apparent that it has two fewer terms than the Lorenz or Rössler models and only a single quadratic nonlinearity ($\dot{x}^2$). So, it is the simplest 3-D dissipative chaotic system with quadratic nonlinearity reported in the literature, as it is proved by Fu and Heidel [50], with a technical correction by Gascon [51]. Later, other simple chaotic jerk systems with quadratic or absolute functions were identified by Sprott (see Table 1 in Ref. [52]). Sprott also found a variety of chaotic jerk functions, the simplest of which have three terms but two nonlinearities. By replacing the term $\dot{x}^2$ with $|\dot{x}|^b$, for b in the range $1 < b < 2$ as well as for larger values of b , Eq. (1) has a chaotic behavior. Munmuangsaen and his co-workers in 2011 revealed many cases with chaotic solutions of Eq. (1), by using various functions in addition to the one with $f(\dot{x}) = \pm \dot{x}^2$ that has been known [53]. Moreover, in 2013, Jafari et al. [54] have found seventeen elementary three-dimensional chaotic flows with quadratic nonlinearities that have the unusual feature of lacking any equilibrium points.

From the circuitry point of view, several attempts to design jerk systems have been presented in literature. In 2005, Yu et al. [55] proposed a novel nonlinear modulating function approach for generating n -scroll chaotic attractors based on a general jerk circuit. Later, Yalcin, presented the use of the Josephson junction in a general jerk circuit, in such a way, that there is no need for synthesizing the nonlinearity toward chaotic n -scroll and hyperchaotic n -scroll hypercube attractors [56]. In 2012, Chunxia et al. [57] presented the theory of the multi-scroll chaotic attractor based on a jerk model, which has been circuitry realized. Next year, a new chaotic jerk circuit, which had been realized using a current-tunable technique, was presented [58]. Later, Ma et al. [20] proposed a feasible feedback scheme, which was used to stabilize the multi-scroll attractors in the jerk circuit, and the controller was realized using mixed Heaviside function. In 2015, Vaidyanathan et al. [59] proposed a six-term 3-D novel jerk chaotic system with two hyperbolic sinusoidal nonlinearities and its circuit realization. The same year another work on a six-term novel 3-D jerk chaotic system with two

Fig. 1 Circuit diagram of the proposed circuit



exponential nonlinearities and its circuit have been presented [59].

In this work, a jerk circuit, which has the same number of terms and similar structure as Eq. (1), is studied. Also, the proposed system contains the hyperbolic sine term as its only nonlinear term. The hyperbolic sine term can be implemented with two antiparallel diodes. The new jerk circuit presents interesting dynamical phenomena such as antimonotonicity and coexisting attractors. Furthermore, a sound encryption scheme, which is based on a random number generator implemented with the proposed jerk system, is presented. The results of NIST-800-22 tests of the random number generator confirm the successful use of the simple chaotic jerk system in the proposed sound encryption scheme.

The rest of the paper is structured as follows. Section 2 deals with the design and the mathematical model of the chaotic jerk circuit, which is derived to investigate the dynamics of the system. The theoretical analysis of system's dynamic characteristics is studied in Sect. 3, while its dynamical properties are presented in Sect. 4. In Sect. 5 a chaotic random number generator based on the proposed jerk system is described. This chaotic random number generator is used on a sound encryption scheme, which is presented in Sect. 6. Finally, the conclusions are summarized in Sect. 7.

2 The proposed circuit

As it is mentioned, in this work a simple nonlinear autonomous circuit is considered (Fig. 1). The circuit consists of resistors, three capacitors and four opera-

tional amplifiers (TL084CN), from which three of them ($U_1 - U_3$) are configured as integrators, while the fourth (U_4) is used as an inverting amplifier. Its nonlinear element consists of two antiparallel diodes connected in the nodes A, B. The current through each of the diodes is described by the following Shockley diode equation:

$$I_D = I_S \left(e^{\frac{v_D}{nV_T}} - 1 \right) \quad (2)$$

where I_S is a reverse bias saturation current, n is a diode ideality factor, V_T is a thermal voltage and v_D is a voltage over the diode. Conventional diodes are made from a variety of semiconductor materials and their ideality factors are not constant [60,61]. By applying Kirchhoff's current law into the node A the following equation is obtained.

$$\begin{aligned} I &= I_1 - I_2 = I_S \left(e^{\frac{v_{AB}}{nV_T}} - 1 \right) - I_S \left(e^{\frac{-v_{AB}}{nV_T}} - 1 \right) \\ &= I_S \left(e^{\frac{v_{AB}}{nV_T}} - e^{\frac{-v_{AB}}{nV_T}} \right) \\ &= 2I_S \sinh \left(\frac{v_{AB}}{nV_T} \right) \end{aligned} \quad (3)$$

because it is known from the theory that $\sinh(x) = (e^x - e^{-x})/2$.

Therefore, by applying the Kirchhoff's laws into the circuit of Fig. 1, its mathematical model given by the system of three differential equations is obtained as:

$$\begin{cases} C_1 \frac{dv_{C1}}{dt} = -\frac{1}{R} v_{C2} \\ C_2 \frac{dv_{C2}}{dt} = -\frac{1}{R} v_{C3} \\ C_3 \frac{dv_{C3}}{dt} = -\frac{1}{R} v_{C1} - \frac{1}{R_b} v_{C3} + \frac{R_a}{R} 2I_S \sinh \left(\frac{v_{C2}}{nV_T} \right) \end{cases} \quad (4)$$

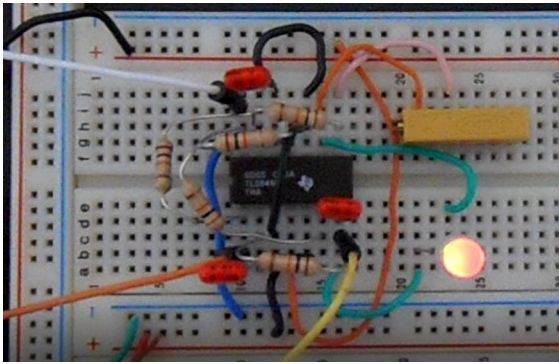


Fig. 2 Photograph of the experimental realization of the proposed circuit of Fig. 1, with a bicolor LED

In system (4), v_{C_1} , v_{C_2} and v_{C_3} are the voltages across the three capacitors C_1 , C_2 and C_3 , respectively, and also $v_{C_2} = v_{AB}$. It is noted that these capacitors have the same values ($C_1 = C_2 = C_3 = C$) in this work. System (4) is rescaled by using dimensionless variables and parameters given by: $x = \frac{v_{C_1}}{nV_T}$, $y = \frac{v_{C_2}}{nV_T}$, $z = \frac{v_{C_3}}{nV_T}$, $\tau = \frac{t}{RC}$, $a = \frac{2R_a I_S}{nV_T}$ and $b = \frac{R}{R_b}$.

As a result, the system (4) is rewritten as:

$$\begin{cases} \frac{dx}{d\tau} = -y \\ \frac{dy}{d\tau} = -z \\ \frac{dz}{d\tau} = -x - bz + a \sinh(y) \end{cases} \quad (5)$$

As seen in (5), the system contains only five terms and it has only one nonlinear term, which is the hyperbolic sine term $\sinh(y)$. This system can be reduced to the jerk form

$$\ddot{x} = -x - b\ddot{x} + a \sinh(-\dot{x}) \quad (6)$$

or by replacing the $\sinh(-\dot{x})$ with $-\sinh(\dot{x})$ the following jerk equation can be obtained.

$$\ddot{x} = -x - b\ddot{x} - a \sinh(\dot{x}) \quad (7)$$

So, system (5) belongs to the family of jerk systems of Eq. (1), in which the term $\dot{x}^2$ has been replaced with the hyperbolic sine term. Therefore, it is one of the simplest nonlinear autonomous systems which has been reported in the literature.

Although the value of the parameter a depends on the diode's characteristics, we can get a desired value of a conveniently by changing the value of the resistor

R_a . For instance, the value of a is fixed as 3.846×10^{-4} by choosing $R_a = 10 \text{ k}\Omega$, $I_S = 1 \text{ nA}$, $V_T = 26 \text{ mV}$ and $n = 2$. It is worth noting that the dynamic behavior of system (5) can be changed by varying the parameter b , which does not affect the diode's equation. In the next sections, the circuit's dynamic behavior is studied by using the following values of elements: $C = 10 \text{ nF}$, $R = 10 \text{ k}\Omega$, R_b : variable resistor and the power supply is $\pm 17 \text{ V}$.

As a different approach in circuit's design, the antiparallel diodes could be replaced with a bicolor LED. A bicolor LED is a single LED package with two LEDs inside, installed in a loop. In this way instead of two common diodes only one element (bicolor LED) has been used in circuit's realization, by decreasing the total number of used elements. Also, by using a bicolor LED, the observer can visually indicate the polarity direction. The experimental realization of the proposed circuit in Fig. 1, with a bicolor LED (red - green) connected at the nodes A, B, is shown in Fig. 2.

Also, in the proposed circuit's realization, the general purpose J-FET quad operational amplifier TL084 with a typical gain bandwidth product at 2 MHz has been used. This feature is satisfactory for the needs of circuit's operation [62, 63], as it is observed from the experimental power spectrum, which is presented in Sect. 4.2. However, for frequency scaling, some limitations may arise [64]. Other electronic devices can also be used to implement this proposed circuit [65], and our proposed design is quite suitable for integrated realization [66].

3 Theoretical analysis of system's dynamical characteristics

3.1 Dissipation—symmetry

According to system (5), the divergence of the system is

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} = -b \cosh(y) \quad (8)$$

where V indicates the phase volume. As the function $\cosh(y) > 0$, for every y , the $\nabla V < 0$, so the state change of the system is bounded; therefore, system (5) is dissipative. So, it converges in the index of the following form

$$\frac{dV}{dt} = e^{-b \cosh(y)t} \quad (9)$$

This means that each volume, containing the trajectories of system (5), will shrink to zero when $t \rightarrow \infty$ with the exponential rate $V_0 e^{-b \cosh(y)t}$. Thus, all the orbits of the system (5) are finally confined to a specific subset of zero volume, and the asymptotic motion of system (5) will be fixed on an attractor of the system [67].

Furthermore, the invariance of system (5) is indicated by the coordinate transformation $(x, y, z) \rightarrow (-x, -y, -z)$. Thus, if (x, y, z) is a solution of system (5) for a specific set of parameters, then $(-x, -y, -z)$ is also a solution for the same parameter set. As a consequence, projected onto the (x, y, z) space, attractors have to be symmetric by inversion with respect to the origin. This symmetry could serve to justify the occurrence of several coexisting attractors in state space.

So, as a conclusion, of the above analysis, the proposed system (5) is dissipative and has coexisting attractors, two very important features in chaotic dynamics.

3.2 Equilibria and stability

The equilibrium points of system (5) can be found by solving

$$\begin{cases} -y = 0 \\ -z = 0 \\ -x + a \sinh(y) - bz = 0 \end{cases} \quad (10)$$

Thus, system (5) has a single equilibrium point $E(0, 0, 0)$. In general, the number of equilibrium points is not equal to the order of the system, that is, the number of the equilibrium points is independent of the order of the system. To linearize the system shown by system (5) at the equilibrium point E , the corresponding Jacobian matrix is expressed by

$$J_E = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ -1 & a & -b \end{bmatrix} \quad (11)$$

Therefore, the characteristic equation of system (5) at the equilibrium point E can be found as:

$$|J_E - \lambda I_D| = \lambda^3 + b\lambda^2 + a\lambda + 1 \quad (12)$$

The eigenvalues can be obtained from (12) to determine system stability. Obviously, the stability of the equilibrium point of system (5) depends on system parameters. By choosing $a = 3.846 \times 10^{-4}$ and $b = 0.7$, the eigenvalues are: $\lambda_1 = -1.2955$, $\lambda_2 = 0.2978 + 0.8266i$ and $\lambda_3 = 0.2978 - 0.8266i$. So E is a saddle focus equilibrium point of index 2. For many chaotic systems, such as the well-known Chua's circuit, saddle focus equilibrium point of index 2 is the premise of scroll motion.

4 Dynamical properties of the system

4.1 Lyapunov exponents and Kaplan-Yorke dimension

As it is known from the theory, the adjacent trajectories of chaotic attractors have shown a tendency of mutual expansion, and Lyapunov exponent is a quantitatively description of mutual repulsion and attraction between trajectories. The Lyapunov exponent of a system is an important feature to judge whether a system is chaotic or not. There are many methods for calculating the Lyapunov exponents. The algorithm of Wolf et al. [68] has been applied in this work for the calculation of system's (5) Lyapunov exponents, with $a = 3.846 \times 10^{-4}$ and $b = 0.7$. The three Lyapunov exponents are $L_1 = 0.21244$, $L_2 = 0$, $L_3 = -1.22543$. The positive L_1 exponent value suggests that the attractor is a strange attractor, and its motion is chaotic. The Kaplan-Yorke dimension [69], which presents the complexity of attractor, is defined by

$$D_{KY} = j + \frac{1}{|L_{j+1}|} \sum_{i=1}^j L_i \quad (13)$$

where j is the largest integer satisfying $\sum_{i=1}^j L_i \geq 0$ and $\sum_{i=1}^{j+1} L_i \leq 0$. The Kaplan-Yorke dimension of system (5) for $a = 3.846 \times 10^{-4}$ and $b = 0.7$ is $D_{KY} = 2.1759$, which indicates that the new system has a fractal dimension and it is proved to be chaotic.

4.2 Time domain waveform, power spectrum and Poincaré map

As shown in Fig. 3, the time domain waveforms of the signals x , y and z , produced by the nonlinear circuit of Fig. 1, which are captured with a digital oscilloscope,

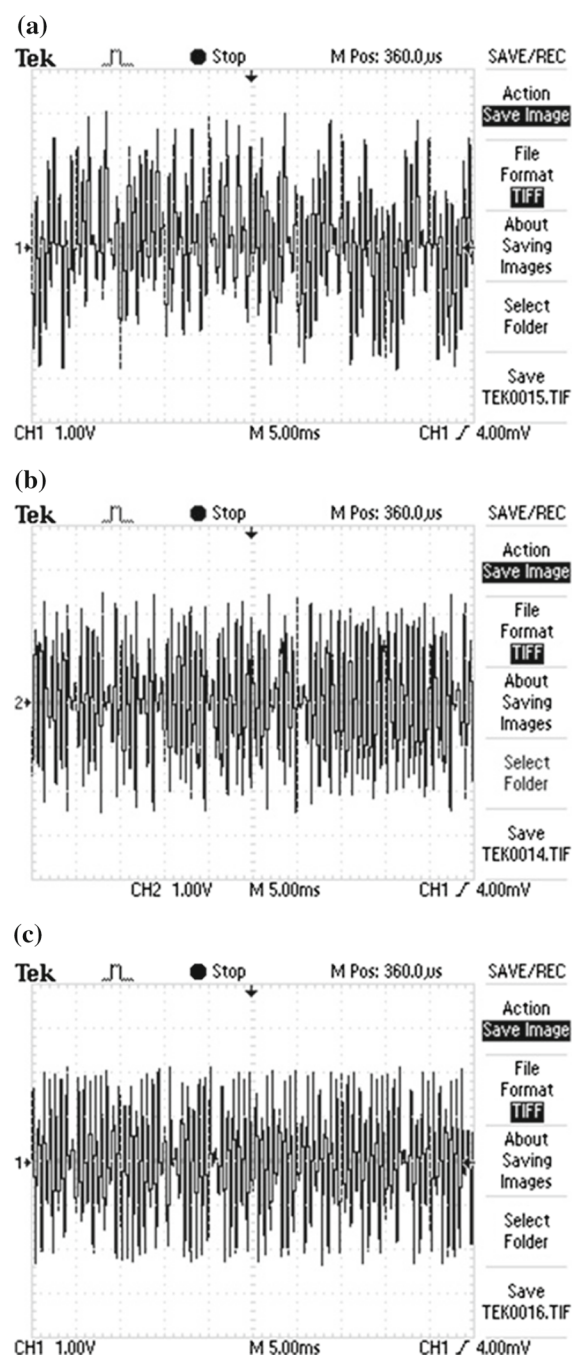


Fig. 3 Experimental time series of variables x , y , z of the proposed circuit

are irregular and unsmooth. The time domain waveforms change in a complicated way, and each of the waveform's amplitude and width are not the same. This feature describes the unification between definiteness

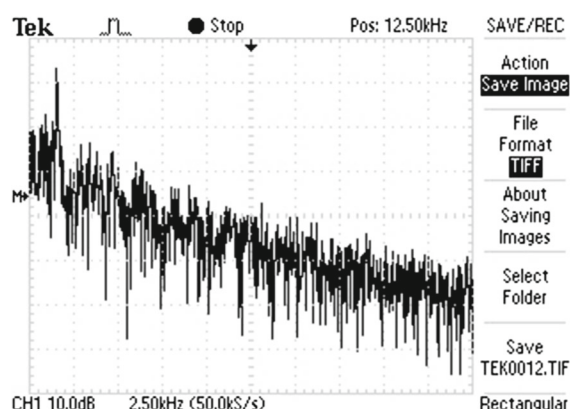


Fig. 4 The experimental power spectrum of the proposed circuit

and randomness, also order and disorder in nonlinear systems.

The experimental power spectrum of the proposed circuit of Fig. 1, is shown in Fig. 4, from which it can be seen that the spectrum of the circuit is continuous. There are peaks in the spectrum and the peaks are connected together, from which its aperiodic characteristics are further demonstrated. It illustrates that circuit of Fig. 1 is a chaotic circuit, and it can be seen that the spectrum is very wide.

As an important analytical technique, Poincaré mapping can reflect the bifurcation and the folding characteristics of chaos. When $b = 0.7$ and $a = 3.846 \cdot 10^{-4}$, one may take $y = 0$ as crossing plane, with $dy/dt > 0$. As shown in Fig. 5, there are some dense points with fractal structure on the cross section and it shows that the system has very rich dynamics characteristics. These features can further explain that the motion of system (5) is chaotic.

4.3 The influence of system's parameter b

In this section, the influence of the proposed system's (5) parameter b to its dynamical behavior, by keeping the value of $a = 3.846 \times 10^{-4}$ with initial conditions $(x_0, y_0, z_0) = (0, 0.1, 0)$, is performed. For the investigation of the proposed circuit's dynamical behavior, system (5) is integrated numerically using the classical fourth-order Runge–Kutta integration algorithm. For each set of parameters used in this work, the time step is always $\Delta t = 0.001$ and the calculations are performed using variables and parameters in extended precision

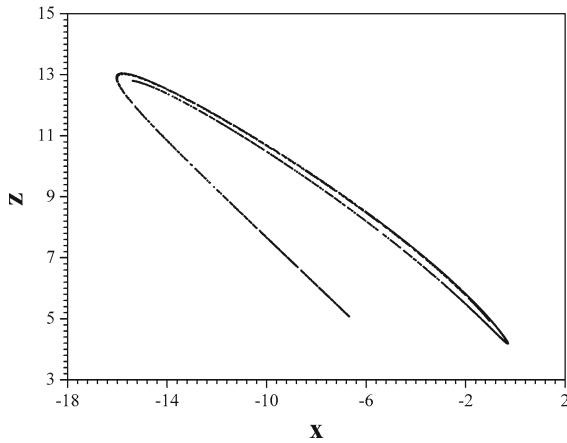


Fig. 5 The Poincaré map of the proposed system (5)

mode. For each parameters setting, the system is integrated for a sufficiently long time and the transient is deleted.

With the variation of system's (5) parameter b , the stability of the system will change; thus, the system will also be in different state. With the help of bifurcation diagram, the Maximal Lyapunov Exponent (MLE) spectrum and the phase diagram, system (5) can be directly analyzed along with the variation of the parameter b .

Firstly, the bifurcation diagram, which is a valuable tool that gives the change of system's dynamic behavior, is used. In this work, the bifurcation diagram of x versus b has been produced when the trajectory crosses the plane $y = 0$ with $dy/dt > 0$, in terms of the control parameter b that is increased (or decreased) in tiny steps in the range $0.3 \leq b \leq 1.5$. Also, the final state at each iteration of the control parameter serves as the initial state for the next iteration. This procedure is more close to the experimental study of circuit's dynamical behavior by using a variable resistor as R_b . In the graph of Fig. 6, two set of data corresponding respectively for increasing (black) and decreasing (red) values of b are superimposed. This strategy represents a simple way to localize the range of values in which the system develops coexisting attractors [67,68], because the system has different initial conditions for the respective values of the control parameter b , in each one of the two superimposed bifurcation diagrams. With this procedure, the phenomenon of coexisting attractors is immerge. Here, the parameter a is kept as $a = 3.846 \cdot 10^{-4}$ and the initial conditions are $(x_0, y_0, z_0) = (0, 0.1, 0)$.

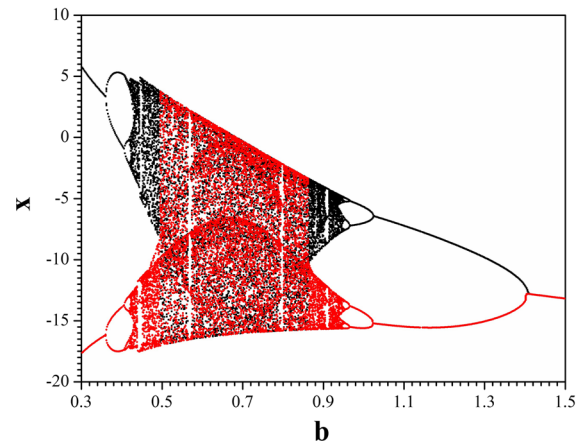


Fig. 6 Bifurcation diagram of system (5), when varying b

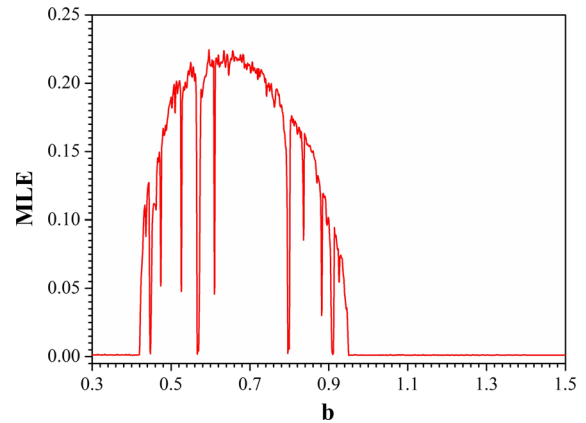


Fig. 7 Maximal Lyapunov exponents (MLE) of system (5), when varying b

As is known that, the MLE determines a notion of predictability of system (5). A positive MLE in the range of $b \in [0.42, 0.95]$ in Fig. 7, except of small windows in which the MLE is equal to zero, is an indication that the system is chaotic. This chaotic behavior is also confirmed by the simulation and experimental phase portraits in Fig. 8, for $b = 0.7$. Moreover, the system displays a periodic state when MLE is equal to zero, for $b < 0.42$, $b > 0.95$ and for the aforementioned small windows inside the chaotic region. As shown in Fig. 7, the results from the MLE diagram regarding system's behavior are consistent with the results produced from the bifurcation diagram of Fig. 6.

Furthermore, from the bifurcation diagrams of Fig. 6, the coexistence behavior of system (5) is illustrated. As the reader can see, the system begins for $b =$

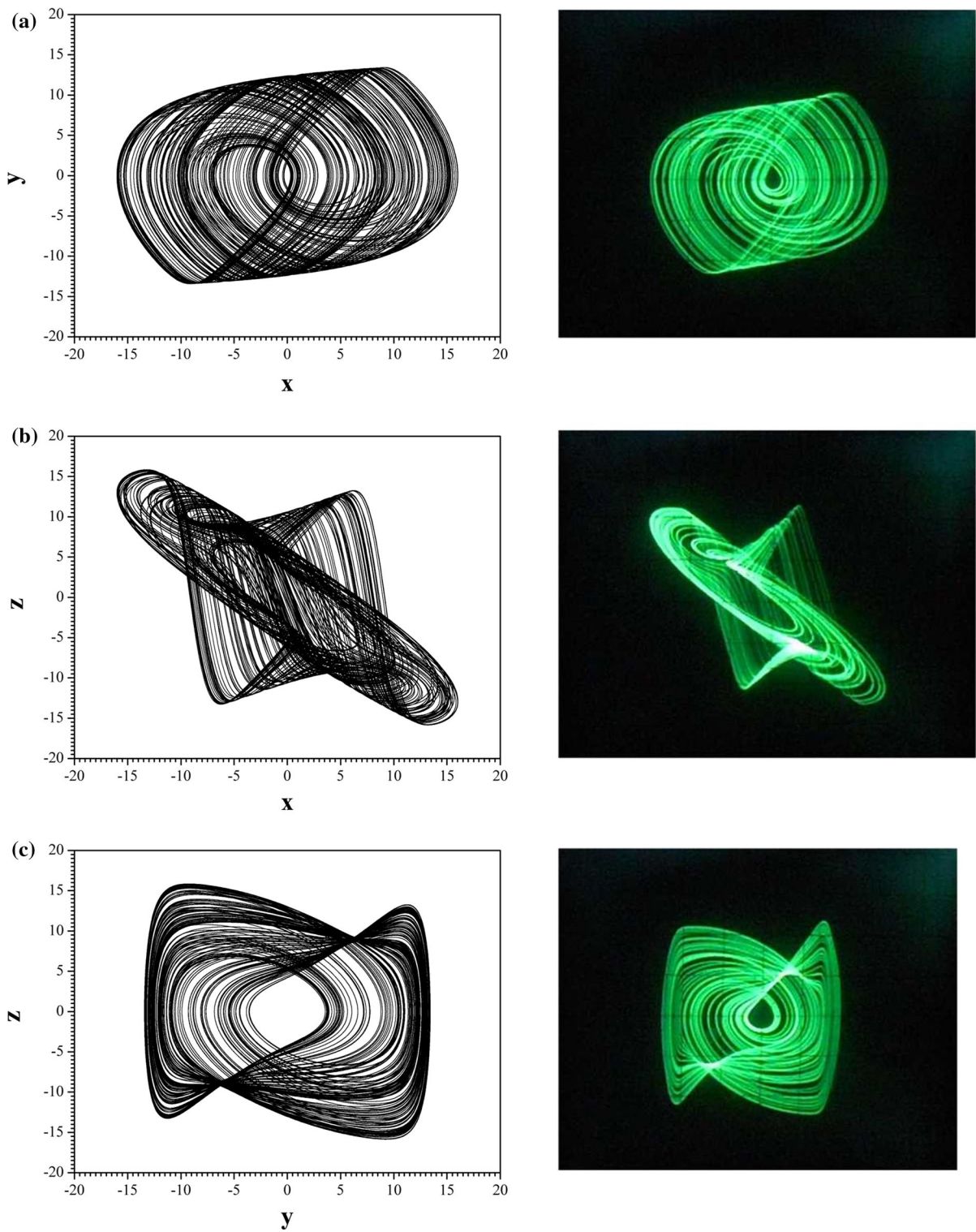


Fig. 8 Simulation and experimental phase portraits of system (5), in **a** (x, y) plane, **b** (x, z) plane and **c** (y, z) plane, for $b = 0.7$ ($X : 1V/div, Y : 1V/div$)

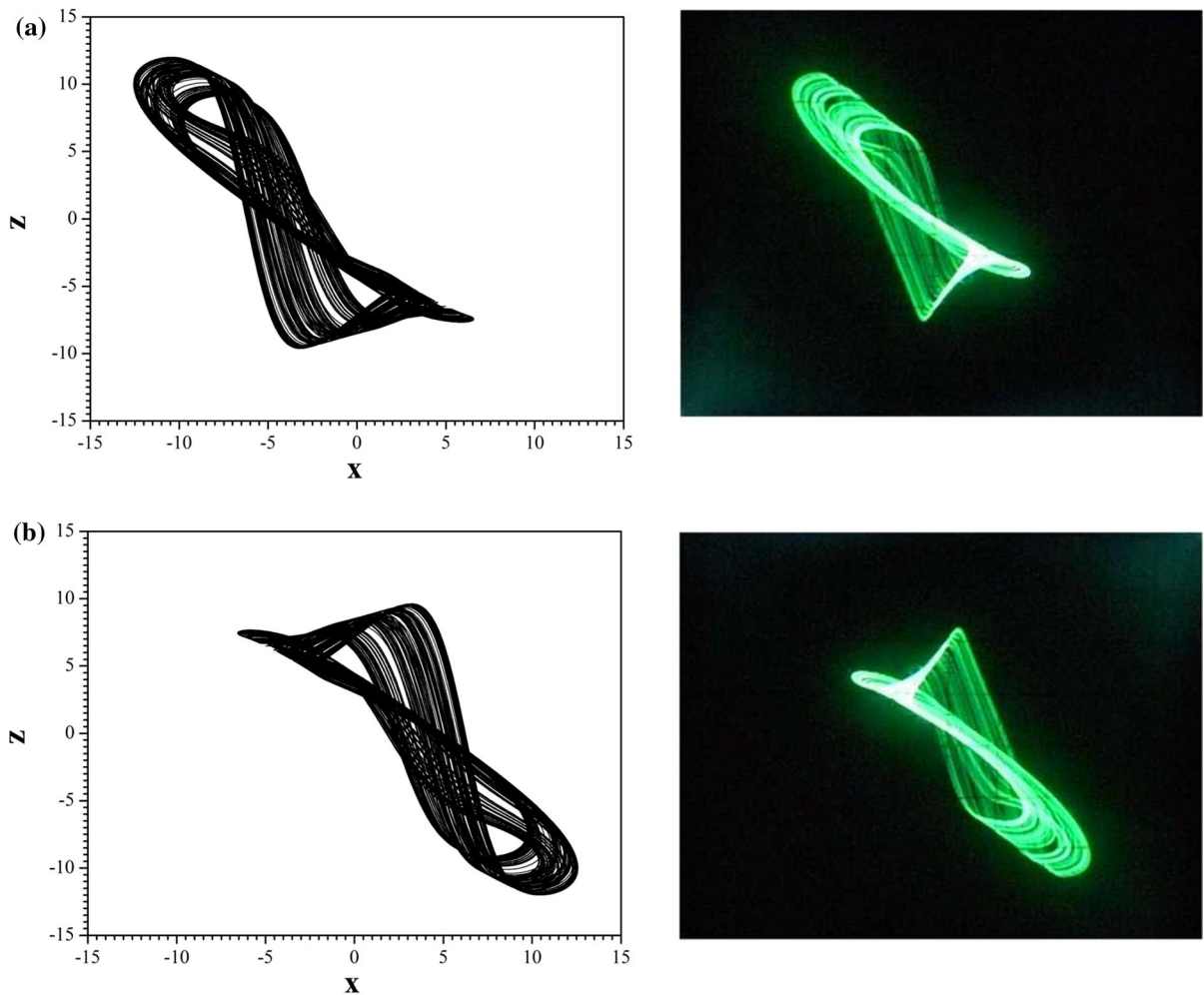


Fig. 9 Simulation and experimental coexisting chaotic attractors, with initial conditions. **a** $(x_0, y_0, z_0) = (0, 0.1, 0)$, **b** $(x_0, y_0, z_0) = (0, -0.1, 0)$, and $b = 0.47$ ($X : 1V/div, Y : 1V/div$)

0.3 from a period-1 state (p-1) but from different values of x and enters to chaos through a period doubling route. In Fig. 9 the simulation and the experimental coexisting chaotic attractors for $b = 0.47$ are depicted.

Also, with a more clear view in the bifurcation diagram of Fig. 6, a second interesting phenomenon concerning system's (5) dynamical behavior can be observed. This is the antimonotonicity, which has been introduced by Dawson et al. [72]. According to this phenomenon, the system enters to chaos with the well-known period doubling route ($p-1 \rightarrow p-2 \rightarrow \dots \rightarrow$ chaos) and exits from the chaos following the reverse period doubling route (chaos $\rightarrow \dots \rightarrow p-2 \rightarrow p-1$). As a result, a shape of a chaotic bubble is formed in the bifurcation diagram.

5 A chaotic random number generator based on the proposed jerk system

Chaos-based encryption has recently become one of the most popular methods in encryption techniques. With developing technology, real-time noise sources and chaotic systems, which have very 'random' and sensitive features and can be easily realized as analog or digital circuits, are today used as Random Number Generators (RNGs) [24, 70–76]. There are many studies already available in the literature concerning RNGs by using chaotic systems [77–79]. Furthermore, chaotic RNGs can be used in many fields such as encryption, data hiding, simulation, modeling, medicine and robotics [21, 80–86].

Fig. 10 The block diagram of the RNG based on the proposed chaotic system (14)

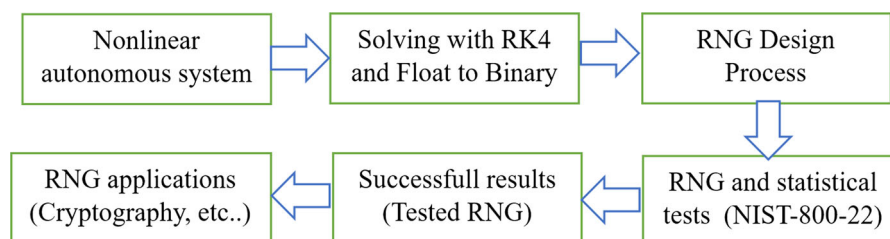


Table 1 RNG NIST-800-22 tests for X , Y and Z outputs

NIST-800-22 tests	P value (X)	P value (Y)	P value (Z)	Result
Frequency (Monobit) test	0.5578	0.1763	0.5974	Successful
Block-frequency test	0.2721	0.5307	0.2087	Successful
Cumulative-sums test	0.8554	0.2130	0.7430	Successful
Runs test	0.6428	0.2543	0.3220	Successful
Longest-run test	0.7557	0.4003	0.8372	Successful
Binary matrix rank test	0.8131	0.3536	0.4501	Successful
Discrete Fourier transform test	0.4246	0.3540	0.2997	Successful
Non-overlapping templates test	0.0004	0.0038	0.0048	Successful
Overlapping templates test	0.1091	0.1830	0.5316	Successful
Maurer's universal statistical test	0.6666	0.3413	0.8691	Successful
Approximate entropy test	0.7873	0.9858	0.0344	Successful
Random excursions test ($x = -4$)	0.1255	0.4307	0.9419	Successful
Random excursions variant test ($x = -9$)	0.5422	0.1313	0.9248	Successful
Serial test-1	0.6819	0.8193	0.9722	Successful
Serial test-2	0.6235	0.8263	0.9028	Successful
Linear-complexity test	0.4461	0.9748	0.8874	Successful

Therefore, in this section, a chaotic RNG is realized by using the proposed jerk system (5), which is used as an entropy source due to its complex and sensitive structure. In more details, for increasing the ‘randomness’ of the produced numbers the amplitude values of the signals x , y and z of the chaotic system are reduced by a linear scaling. As can be seen in Fig. 8, the signals, x , y and z take values in the interval of $(-15, 15)$. So, by letting $X = x/4$, $Y = y/4$ and $Z = z/4$ the scaled system becomes

$$\begin{cases} \frac{dX}{dt} = -Y \\ \frac{dY}{dt} = -Z \\ \frac{dZ}{dt} = -X - bZ + \frac{a \sinh(4Y)}{4} \end{cases} \quad (14)$$

Figure 10 depicts, step by step, the block diagram which is followed on the design of the chaotic RNG in MATLAB. The basic procedure in the RNG design is the discretization of the nonlinear autonomous system

(14), which is done by using the fourth-order Runge–Kutta algorithm, which is more preferable in regard to other methods, as it provides more sensitive discretization.

Because of its sensitivity feature, numbers gathered from a continuous time chaotic system discretized by RK4 algorithm are at first derived as float number type. So, in order to receive more successful test results in random number generation, as in the second step seen on the block diagram of Fig. 10, float number types must be converted to binary number one.

As the used chaotic system (14) is a three-dimensional dynamical system, three different RNG can take place at the same time. For faster random number generation, in this article, X , Y , Z outputs were used separately. Also, 32 bits, which are the least bits binary numbers found for each output (X , Y and Z) were used in the proposed RNG.

In order to assess the performance of the generated random numbers, randomness test with internationally highest standards like NIST-800-22 is used [87]. NIST-800-22 include 16 different tests, like frequency, mono-bit, runs, binary matrix rank, serial and random excursions tests. At least 1 Mbit data set, in other words generated random number arrays, is required for NIST-800-22 tests. Numbers that proved successful in such tests can be considered safe to be used in necessary scientific or engineering applications.

If successful results cannot be obtained on NIST-800-22 tests, randomness can be increased among numbers by using logical operators like XOR or by changing the chosen bit. However, in this work, different random numbers were obtained for each X , Y and Z output and tests were run. The low bits binary numbers found for each output (X , Y and Z) were used for RNG. Last 8 bits, last 16 bits and last 4 bits, respectively, were used for X , Y and Z . The random numbers found here were put through NIST-800-22 randomness tests processes, and successful results were received for each X , Y and Z outputs. Table 1 exhibits the information of NIST-800-22 tests results for the proposed chaotic RNG.

6 A sound encryption application with the RNG based on the jerk system

In this section, an encryption implementation was performed on a sound data with RNGs designed with the scaled nonlinear autonomous system (14). A sound file of 101150 data was used for sound encryption. Figure 11 shows the block diagram needed for encryption and decryption. On the block diagram in Fig. 11, keys made up of '0's and '1's are needed for encryption. These keys are tested as random numbers. Keys are derived as random numbers from the scaled nonlinear autonomous system. As the sound data to be encrypted are not in binary format, some conversion must be done. Sound data in float number type must be converted to binary number format for encryption. Keys in binary number format and the sound data to be encrypted were only encrypted with XOR logical operator.

For the decryption of the encrypted data, the same keys, which are used in encryption, need to be regenerated. For this reason, one has to know the initial values as well as the values of parameters of the chaotic system (14). So, by regenerating the exact random numbers sequence, the encrypted text data will be decrypted

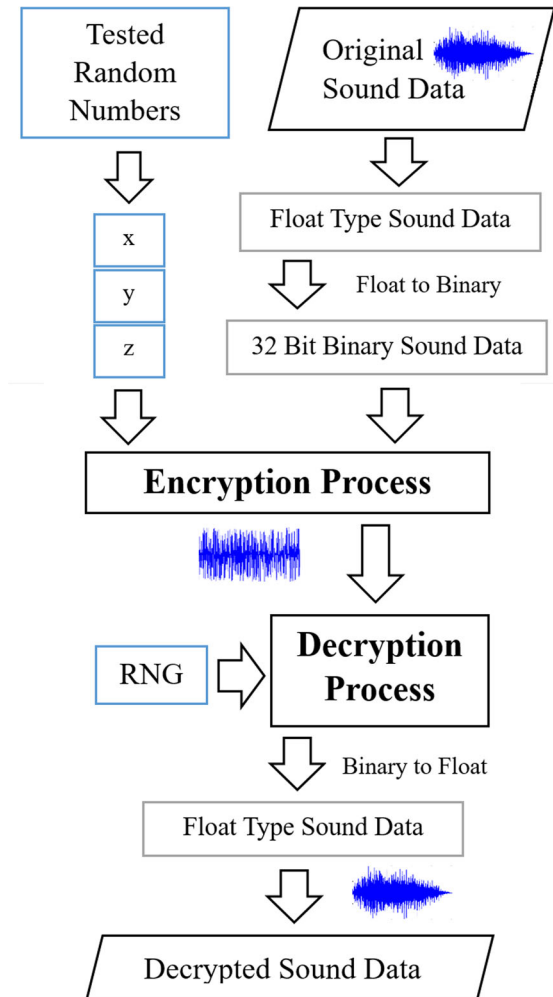


Fig. 11 Encryption and decryption block diagram

by using the XOR process again between the keys in binary format and the encrypted data.

The original sound that is to be encrypted is given in Fig. 12. The sound data in 'float' format are converted to 32 bit binary format. It is needed to have $101150 \times 32 = 3236800$ binary number arrays which are generated from the RNG to encrypt the converted binary data. The converted binary data are encrypted with the binary number arrays which are consisted of 0s and 1s. The encrypted binary array is converted back to float format. The encrypted sound is given in Fig. 13. As it can be seen from Fig. 13, encrypted sound data are very complex and its amplitude values very big.

The decrypted sound is given in Fig. 14. As it can be seen from Figs. 12 and 14, there is no difference

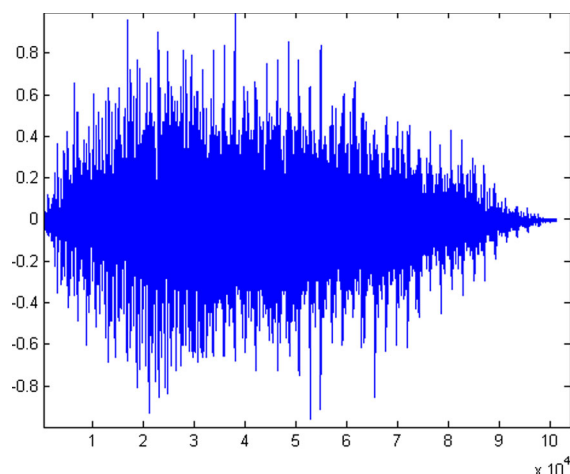


Fig. 12 The original sound data

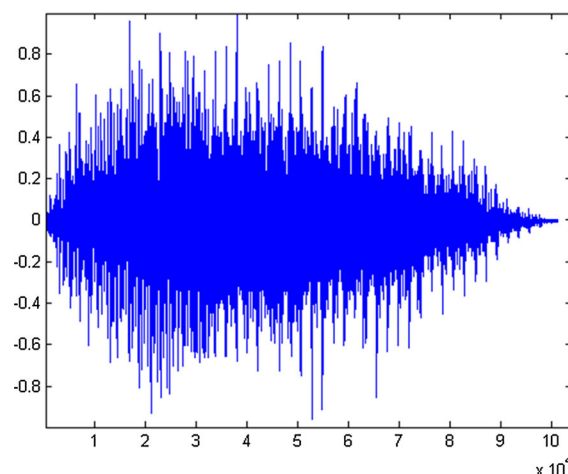


Fig. 14 The decrypted sound data

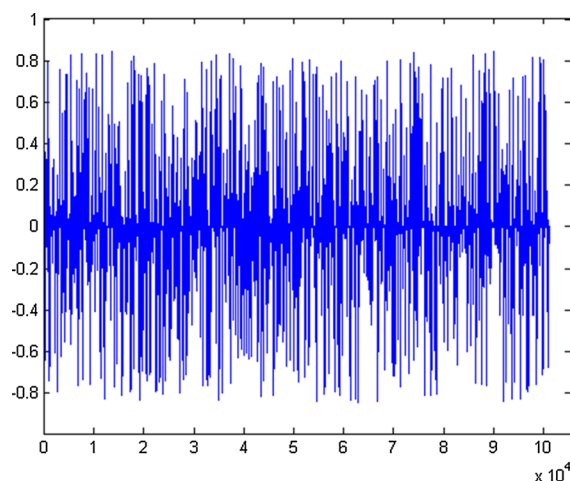


Fig. 13 The encrypted sound data

between the original and the decrypted sound. The success in the encryption is ensured by using RNG number array which successfully passes NIST-800-22 tests. Also, the time elapsed for encryption of 101150 binary number array with XOR operation is 84.4 ms, while the time elapsed for decryption is 85.5 ms. The requirement of high speed in the encryption and decryption process are succeeded by using a simple chaotic system and a logic operation of 'XOR'.

7 Conclusion

In this paper, a very simple chaotic autonomous circuit has been presented. The circuit has five terms and

only one nonlinear term, which is the hyperbolic sine term. This nonlinear term can be implemented with two antiparallel diodes or with a bicolor LED as it was presented. The dynamical system which described the nonlinear autonomous circuit has presented interesting phenomena from the nonlinear theory, such as a period doubling route to chaos, antimonotonicity and coexisting attractors. Also, for confirming the practical usefulness of the proposed simple chaotic autonomous circuit, a sound encryption scheme, which is based on a random number generator implemented with the proposed system, was presented. The results of NIST-800-22 tests of the random number generator, as well as the encryption and decryption process of the sound, were successful. Finally, the proposed circuit, due to its simplicity and its rich dynamical behavior, will be the base in future works related with synchronization and secure communication schemes.

References

1. Chen, G.: Controlling Chaos And Bifurcations In Engineering Systems. CRC Press, Boca Raton (1999)
2. Chen, G., Ueta, T.: Chaos In Circuits And Systems. World Scientific, Singapore (2002)
3. Koyuncu, I., Ozcerit, A.T., Pehlivan, I.: An analog circuit design and FPGA-based implementation of the Burke-Shaw chaotic system. J. Optoelectron. Adv. Mater. **7**, 635–638 (2013)
4. Itoh, M., Chua, L.O.: Memristor oscillators. Int. J. Bifurc. Chaos **18**, 3183–3206 (2008)

5. Buscarino, A., Fortuna, L., Frasca, M., Gambuzza, L.V.: Memristive chaotic circuits based on cellular nonlinear networks. *Int. J. Bifurc. Chaos* **22**, 1250070 (2012)
6. Gopal, S., Lai, Y.C.: Inducing chaos in MOSFET-based electronic circuits. *Circ. Syst. Signal Process.* **28**, 535–545 (2009)
7. Borah, M., Singh, P.P., Roy, B.K.: Improved chaotic dynamics of a fractional-order system, its chaos-suppressed synchronisation and circuit implementation. *Circ. Syst. Signal Process.* **35**, 1871–1907 (2016)
8. Newcom, R.W., El-Leithy, N.: Chaos generation using binary hysteresis. *Circ. Syst. Signal Process.* **5**, 321–341 (1986)
9. Azar, A.T., Volos, C., Gerodimos, N.A., Tombras, G.S., Pham, V.T., Radwan, A.G., Vaidyanathan, S., Ouannas, A., Munoz-Pacheco, J.M.: A novel chaotic system without equilibrium: Dynamics, synchronization and circuit realization. *Complexity* **2017** (2017). doi:[10.1155/2017/7871467](https://doi.org/10.1155/2017/7871467)
10. Cuomo, K.M., Oppenheim, A.V.: Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.* **71**, 65–68 (1993)
11. Liao, T.L., Tsai, S.H.: Adaptive synchronization of chaotic systems and its application to secure communications. *Chaos Soliton Fract.* **11**, 1387–1396 (2000)
12. Kolumban, G., Kennedy, M.P., Chua, L.O.: The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization. *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.* **45**, 1129–1140 (1998)
13. Tam, W.M., Chi, K.T.: A near-optical noncoherent chaos-based communication scheme. *Circ. Syst. Signal Process.* **24**, 675–687 (2005)
14. Kaddoum, G., Lawrance, A.J., Charge, P., Roviras, D.: Chaos communication performance: theory and computation. *Circ. Syst. Signal Process.* **30**, 185–208 (2011)
15. Azar, A.T., Vaidyanathan, S.: *Chaos Modeling And Control Systems Design, Studies In Computational Intelligence*, vol. 581. Springer, Berlin (2015)
16. Vaidyanathan, S., Azar, A.T., Rajagopal, K., Alexander, P.: Design and SPICE implementation of a 12-term novel hyperchaotic system and its synchronization via active control. *Int. J. Model. Identif. Contr.* **23**, 267–277 (2015)
17. Zhou, J., Chen, T., Xiang, L.: Chaotic lag synchronization of coupled delayed neural networks and its applications in secure communication. *Circ. Syst. Signal Process.* **24**, 599–613 (2005)
18. Grassi, G., Mascolo, S.: Synchronizing high dimensional chaotic systems via eigenvalue placement with application to cellular neural networks. *Int. J. Bifurc. Chaos* **9**, 705–711 (1999)
19. Chua, L.O., Yang, L.: Cellular neural networks: applications. *IEEE Trans. Circuits Syst.* **35**, 1273–1290 (1988)
20. Ma, J., Wu, X., Chu, R., Zhang, L.: Selection of multi-scroll attractors in Jerk circuits and their verification using Pspice. *Nonlinear Dyn.* **76**, 1951–1962 (2014)
21. Wu, X., Ma, J., Yuan, L., Liu, Y.: Simulating electric activities of neurons by using PSPICE. *Nonlinear Dyn.* **75**, 113–126 (2014)
22. Li, F., Liu, Q., Guo, H., Zhao, Y., Tang, J., Ma, J.: Simulating the electric activity of FitzHugh-Nagumo neuron by using Josephson junction model. *Nonlinear Dyn.* **69**, 2169–2179 (2012)
23. Ren, G., Xu, Y., Wang, C.: Synchronization behavior of coupled neuron circuits composed of memristors. *Nonlinear Dyn.* doi:[10.1007/s11071-016-3283-2](https://doi.org/10.1007/s11071-016-3283-2) (2017)
24. Yalcin, M.E., Suykens, J.A.K., Vandewalle, J.: True random bit generation from a double-scroll attractor. *IEEE Trans. Circuits Syst. I, Reg. Pap.* **51**, 1395–1404 (2004)
25. Bernstein, G.M., Lieberman, M.A.: Secure random number generation using chaotic circuits. *IEEE Trans. Circuits Syst.* **37**, 1157–1164 (1990)
26. Arena, P., Fortuna, L., Frasca, M.: Attitude control in walking hexapod robots: an analogic spatio-temporal approach. *Int. J. Circ. Theory Appl.* **30**, 349–362 (2002)
27. Nakamura, Y., Sekiguchi, A.: The chaotic mobile robot. *IEEE Trans. Robot. Autom.* **17**, 898–904 (2001)
28. Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N.: A chaotic path planning generator for autonomous mobile robots. *Robot. Auton. Syst.* **60**, 651–656 (2012)
29. Bouali, S., Buscarino, A., Fortuna, L., Frasca, M., Gambuzza, L.V.: Emulating complex business cycles by using an electronic analogue. *Nonlinear Anal. Real* **13**, 2459–2465 (2012)
30. Tacha, O.I., Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N., Vaidyanathan, S., Pham, V.T.: Analysis, adaptive control and circuit simulation of a novel nonlinear finance system. *Appl. Math. Comput.* **276**, 200–217 (2016)
31. Linsay, P.S.: Period doubling and chaotic behavior in a driven anharmonic oscillator. *Phys. Rev. Lett.* **47**, 1349–1352 (1981)
32. Deane, J.H.: Modeling the dynamics of nonlinear inductor circuits. *IEEE Trans. Magn.* **30**, 2795–2801 (1994)
33. Lakshmanan, M., Murali, K.: Experimental chaos from non-autonomous electronic circuits. *Philos. Trans. A Math. Phys. Eng. Sci.* **353**, 33–46 (2014)
34. Lindberg, E., Murali, K., Tamasevicius, A.: The smallest transistor-based nonautonomous chaotic circuit. *IEEE Trans. Circuits Syst. II, Expr. Briefs* **52**, 661–664 (2005)
35. Tchitnga, R., Fotsin, H.B., Nana, B., Fotso, P.H.L., Wofo, P.: Hartley's oscillator: the simplest chaotic two-component circuit. *Chaos Soliton Fract.* **45**, 306–313 (2012)
36. Pham, V.T., Buscarino, A., Fortuna, L., Frasca, M.: Simple memristive time-delay chaotic systems. *Int. J. Bifurc. Chaos* **23**, 1350073 (2013)
37. Muthuswamy, B., Chua, L.O.: Simplest chaotic circuit. *Int. J. Bifurc. Chaos* **20**, 1567–1580 (2010)
38. Barboza, R., Chua, L.O.: The four-element Chua's circuit. *Int. J. Bifurc. Chaos* **18**, 943–955 (2008)
39. Srisuchinwong, B., Munmuangsaen, B.: Four current-tunable chaotic oscillators in set of two diode-reversible pairs. *Electron. Lett.* **48**, 1051–1053 (2012)
40. San-Um, W., Suksiri, B., Ketthong, P.: A Simple RLCC-Diode-opamp chaotic oscillator. *Int. J. Bifurc. Chaos* **24**, 1450155 (2014)
41. Piper, J.R., Sprott, J.C.: Simple autonomous chaotic circuits. *IEEE Trans. Circuits Syst. II, Exp. Briefs* **57**, 730–734 (2010)
42. Tamasevicius, A., Mykolaitis, G., Pyragas, V., Pyragas, K.: A simple chaotic oscillator for educational purposes. *Eur. J. Phys.* **26**, 61–63 (2005)

43. Lorenz, E.N.: Deterministic nonperiodic flow. *J. Atmos. Sci.* **20**, 130–141 (1963)
44. Rossler, O.E.: An equation for continuous chaos. *Phys. Lett. A* **57**, 397–398 (1976)
45. Rossler, O.E.: Continuous chaos—four prototype equations. *Ann. NY Acad. Sci.* **316**, 376–392 (1979)
46. Sprott, J.C.: Some simple chaotic flows. *Phys. Rev. E* **50**, R647–R650 (1994)
47. Schot, S.H.: Jerk: the time rate of change of acceleration. *Am. J. Phys.* **46**, 1090–1094 (1978)
48. Sprott, J.C.: Some simple chaotic jerk functions. *Am. J. Phys.* **65**, 537–543 (1997)
49. Sprott, J.C.: Simplest dissipative chaotic flow. *Phys. Lett. A* **228**, 271–274 (1997)
50. Fu, Z., Heidel, J.: Non-chaotic behavior in three-dimensional quadratic systems. *Nonlinearity* **10**, 1289–1303 (1997)
51. Fu, Z., Heidel, J.: Non-chaotic behaviour in three-dimensional quadratic systems. *Nonlinearity* **12**, 739 (1999)
52. Sprott, J.C.: Simple chaotic systems and circuits. *Am. J. Phys.* **68**, 758–763 (2000)
53. Munmuangsaen, B., Srisuchinwong, B., Sprott, J.C.: Generalization of the simplest autonomous chaotic system. *Phys. Lett. A* **375**, 1445–1450 (2011)
54. Jafari, S., Sprott, J.C., Golpayegani, S.M.R.H.: Elementary quadratic chaotic flows with no equilibria. *Phys. Lett. A* **377**, 699–702 (2013)
55. Yu, S., Lu, J., Leung, H., Chen, G.: Design and implementation of n-scroll chaotic attractors from a general jerk circuit. *IEEE Trans. Circuits Syst. I, Reg. Pap.* **52**, 1459–1476 (2005)
56. Yalcin, M.E.: Multi-scroll and hypercube attractors from a general jerk circuit using Josephson junctions. *Chaos Soliton Fract.* **34**, 1659–1666 (2007)
57. Chunxia, L., Jie, Y., Xiangchun, X., Limin, A., Yan, Q., Yongqing, F.: Research on the multi-scroll chaos generation based on Jerk mode. *Proced. Eng.* **29**, 957–961 (2012)
58. Srisuchinwong, B., Nopchinda, D.: Current-tunable chaotic jerk oscillator. *Electron. Lett.* **49**, 587–589 (2013)
59. Vaidyanathan, S., Volos, C.K., Pham, V.T., Madhavan, K., Idowu, B.A.: Adaptive backstepping control, synchronization and circuit simulation of a 3-D novel jerk chaotic system with two hyperbolic sinusoidal nonlinearities. *Arch. Control Sci.* **24**, 257–285 (2014)
60. Schubert, E.F.: *Light Emitting Diodes*. Cambridge University Press, Cambridge (2006)
61. Rhderick, E.H., Williams, R.: *Metal-semiconductor Contacts*. Clarendon Press, Oxford (1988)
62. Franco, S.: *Design with Operational Amplifiers and Analog Integrated Circuits*. McGraw-Hill Series in Electrical and Computer Engineering. McGraw-Hill Companies, NY (2015)
63. Clayton, G.B., Winder, S.: *Operational Amplifiers*. Newnes, Oxford (2003)
64. Munoz-Pacheco, J.M., Tlelo-Cuautle, E., Toxqui-Toxqui, I., Sanchez-Lopez, C., Trejo-Guerra, R.: Frequency limitations in generating multi-scroll chaotic attractors using CFOAs. *Int. J. Electron.* **101**, 1559–1569 (2014)
65. Trejo-Guerra, R., Tlelo-Cuautle, E., Carbajal-Gmez, V.H., Rodriguez-Gomez, G.: A survey on the integrated design of chaotic oscillators. *Appl. Math. Comput.* **219**, 5113–5122 (2013)
66. Trejo-Guerra, R., Tlelo-Cuautle, E., Jimenez-Fuentes, J.M., Snchez-Lpez, C., Muoz-Pacheco, J.M., Espinosa-Flores-Verdad, G., Rocha-Prez, J.M.: Integrated circuit generating 3-and 5-scroll attractors. *Commun. Nonlinear Sci.* **17**, 4328–4335 (2012)
67. Argyris, J., Faust, G., Haase, M., Friedrich, R. (eds.): *Dynamical systems with dissipation. In: An Exploration of Dynamical Systems and Chaos*. Springer, Berlin, pp. 189–298 (2015)
68. Wolf, A., Swift, J.B., Swinney, H.L., Vastano, J.A.: Determining Lyapunov exponents from a time series. *Phys. D* **16**, 285–317 (1985)
69. Frederickson, P., Kaplan, J.L., Yorke, E.D., Yorke, J.A.: The Liapunov dimension of strange attractors. *J. Differ. Equ.* **49**, 185–207 (1983)
70. Pisarchik, A.N., Feudel, U.: Control of multistability. *Phys. Rep.* **540**, 167–216 (2014)
71. Ma, J., Wu, F., Ren, G., Tang, J.: A class of initials-dependent dynamical systems. *Appl. Math. Comput.* **298**, 65–76 (2017)
72. Dawson, S.P., Grebogi, C., Yorke, J.A., Kan, I., Kocak, H.: Antimonotonicity: Inevitable reversals of period-doubling cascades. *Phys. Lett. A* **163**, 249–254 (1992)
73. Beirami, A., Nejati, H., Ali, Wh.: Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator. *Electron. Lett.* **48**, 1537–1538 (2012)
74. Zhao, L., Liao, X., Xiao, D., Xiang, T., Zhou, Q., Duan, S.: TRNG from mobile telephone photo based on chaotic cryptography. *Chaos Soliton Fract.* **42**, 1692–1699 (2009)
75. Ergun, S., Ozoguz, S.: Truly random number generators based on a non-autonomous chaotic oscillator. *AEU-Int. J. Electron. C.* **61**, 235–242 (2007)
76. Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N.: Image encryption process based on chaotic synchronization phenomena. *Signal Process.* **93**, 1328–1340 (2013)
77. Akgul, A., Calgan, H., Koyuncu, I., Pehlivan, I., Istanbul, A.: Chaos-based engineering applications with a 3D chaotic system without equilibrium points. *Nonlinear Dyn.* doi:[10.1007/s11071-015-2501-7](https://doi.org/10.1007/s11071-015-2501-7) (2016)
78. Cavusoglu, U., Akgul, A., Kacar, S., Pehlivan, I., Zengin, A.: A novel chaos-based encryption algorithm over TCP data packet for secure communication. *Secur. Commun. Netw.* doi:[10.1002/sec.1414](https://doi.org/10.1002/sec.1414) (2016)
79. Akgul, A., Moroz, I., Pehlivan, I., Sundarapandian, V.: A new four-scroll chaotic attractor and its engineering applications. *Optik* **127**(13), 5491–5499 (2016)
80. Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N.: Fingerprint images encryption process based on a chaotic true bits generator. *Int. J. Multimed. Intell. Secur.* **1**, 320–335 (2010)
81. Caponetto, R., Fortuna, L., Fazzino, S., Xibilia, M.G.: Chaotic sequences to improve the performance of evolutionary algorithms. *IEEE Trans. Evolut. Comput.* **7**, 289–304 (2003)
82. Alatas, B.: Chaotic bee colony algorithms for global numerical optimization. *Expert Syst. Appl.* **37**, 5682–5687 (2010)
83. Morse, M.L., Beem, L.W.: Benefits of Reiki therapy for a severely neutropenic patient with associated influences on a true random number generator. *J. Altern. Complement. Med.* **17**, 1181–1190 (2011)

84. Volos, C.K., Kyprianidis, I.M., Stouboulos, I.N.: Motion control of robots using a chaotic truly random bits generator. *J. Eng. Sci. Technol. Rev.* **5**, 6–11 (2012)
85. Maysaa, A., Iman, Q.: Speech encryption using chaotic map and blowfish algorithms. *J. Basrah Res.* **39**, 68–76 (2013)
86. Akgul, A., Kacar, S., Pehlivan, I.: Audio data encryption with single and double dimension discrete-time chaotic systems. *Turkish Online J. Sci. Technol.* **5**, 14–23 (2015)
87. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 (2010)